

**A Summary for Computer Forensic Professionals of the  
Electronically Stored Evidence (ESI) Amendments to the  
Federal Rules of Civil Procedure, December 1, 2006**

Brian Dykstra  
<http://www.virtualwar.com>  
December 3, 2006

1. What changed? .....	3
2. Jargon: .....	3
3. What is the history of the changes? .....	3
4. What areas of the Federal Rules of Civil Procedure actually changed? .....	3
Rule 16(b) Pretrial Conferences: Scheduling Management .....	3
Rule 26(a) General Provisions Governing Discovery: Duty of Disclosure .....	4
Rule 26(b)(2) Two Tiered Discovery: Data that is Not Reasonably Accessible .....	4
Rule 26(b)(5) Claims of Privilege or Protection After Production .....	4
Rule 26(f) Conference of Parties: Planning for Discover .....	5
Rule 33(d) Option to Produce Business Records .....	5
Rule 34(a) Scope .....	5
Rule 34(b) Procedure .....	6
Rule 37(f) Electronically Stored Information .....	6
Rule 45 Subpoena.....	6
5. What should a company do if something happens?.....	7
6. What mistakes can be avoided? .....	7
7. What can companies do in advance? .....	8
8. What about data on personally owned computer, PDAs, cellphones, etc. ....	8
References and Acknowledgements.....	9

## 1. What changed?

Effective December 1, 2006, there was comprehensive reform amended to the Federal Rules of Civil Procedure designed to provide a uniform approach to e-discovery in federal courts. This is the first time these particular rule have changed since 1970.

## 2. Jargon:

- ESI - Electronically Stored Information - New term created by the Advisory Committee
- EED - Electronic Evidence Discovery (e-discovery)
- EDD - Electronic Data Discovery

## 3. What is the history of the changes?

In 1999 the Discovery Subcommittee of the US Judicial Conference Rules Advisory Committee was tasked with identifying e-discovery rules that were of concern.

By 2003 the individuals working for the Advisory Committee had pulled all the information together to start making new rules.

In August 2004, the Advisory Committee published a package of e-discovery proposals to address the key issues.

In, January and February 2005, public hearings were held in San Francisco, Dallas and Washington, DC.

In April 2005, the Advisory Committee adopted a final package of e-discovery amendments.

The US Judicial Conference and the US Supreme Court both provided favorable recommendations on the final amendments and they were approved by the Standing Committee.

On December 1, 2006 the changes were made to the existing Federal Rules of Civil Procedure. These were amendments to existing law NOT new laws.

## 4. What areas of the Federal Rules of Civil Procedure actually changed?

***Rule 16(b) Pretrial Conferences: Scheduling Management*** alerts the court to the need to address e-discovery issues early in the litigation if discovery of ESI (Electronically Stored Information) is expected. Specifically 90 days after the appearance of the defendant and within 120 days after the complaint has been served to the defendant.

**For Computer Forensic Professionals:**

- The schedule includes the time allotted for disclosure and the extent of discovery
- Provisions for disclosure or discovery of ESI
- Any agreement of privilege or protection
- The date or dates for pretrial conferences
- Anything else that seems appropriate

***Rule 26(a) General Provisions Governing Discovery: Duty of Disclosure*** without waiting for a discovery request a party must provide:

- name, address and telephone number of individuals likely to have discoverable evidence
- a copy of, or a description of that may be used to support claims or defenses

***Rule 26(b)(2) Two Tiered Discovery: Data that is Not Reasonably Accessible***

- The court can limit the number or length of depositions
- A party is not required to provide discovery of ESI from sources the party identifies as not reasonably accessible because of undue burden or cost - The party might be required to show why the ESI is not reasonably accessible and the court can reject the claim and order discovery
- The discovery will be limited if the court determines it is unreasonably duplicative; if the data is obtainable from a more reasonable source; if the burden or expense outweighs the likely benefits

**For Computer Forensic Professionals:**

- If the parties cannot agree on reasonable search and discovery the court will decide
- Even after it is shown that a source of ESI is not reasonably accessible a party by showing good cause that balance the cost and the potential benefits. There is a set of criteria that must be met for this
- The limitations are commonly referred to as "Two Tiered Discovery". Essentially the Advisory Committee recognizing that some data is easy to retrieve and some data is very hard, expensive or impossible to retrieve.

***Rule 26(b)(5) Claims of Privilege or Protection After Production***

"privileged information" usually discussions between individuals and their attorneys

"privilege waiver" when data that is privileged is disclosed to the other party

"claw back" the ability of a party to take back privileged or protected information that was inadvertently disclosed during e-discovery

The parties will have established criteria for what is privileged and if a claim of privilege is made after e-discovery data has been provided to the receiving party they must return, sequester or destroy the information. They may of course challenge the "claw back".

**For Computer Forensic Professionals:**

- The disputed information must be preserved by the producing party pending the court's ruling regardless **\*\*Liability ALERT\*\***
- "embedded data" and "metadata" could contain privileged information not readily viewable to the normal viewer of a file in print or on a screen
- Lawyers usually try to avoid accessing other parties privileged information to avoid potential disputes

**Rule 26(f) Conference of Parties: Planning for Discover** the parties must as soon as practical or at least 21 days before a scheduling conference or scheduling order is due, confer to make arrangements for disclosures and discuss issues related to preserving discoverable information and develop a proposed discovery plan.

The parties must discuss the balance between preservation and the need to continue the routine operations of the organization. The parties should agree on reasonable preservation steps.

**For Computer Forensic Professionals:**

- Preservation of dynamic data must be addressed to avoid the risk of future disputes

**Rule 33(d) Option to Produce Business Records** some records may exist only in a specific electronic format on a specific electronic information system. A party must be given "reasonable opportunity to examine, audit, or inspect the information". If sensitive interests of privacy or confidentiality issues are involved the responding party may need to derive or provide answers from these systems. Rule 33(d) also requires the responding party to locate and identify requested data "as readily as the party served".

**For Computer Forensic Professionals:**

- Unique data stores should be identified as early as possible and plans developed for handling of the data

**Rule 34(a) Scope** acknowledges that traditional paper documents are different from ESI even though data may be in both forms. Further the rule specifies that data must be translated into a reasonably usable form. If the data

cannot be translated the party must allow access to the ESI for inspection, measuring, surveying, photographing, testing or sampling.

#### **For Computer Forensic Professionals:**

- It is in the clients best interests to provide the data requested in an agreed upon format. Special attention should be given to database information or highly specialized data such as CAD/CAM

**Rule 34(b) Procedure** permits the requesting party to specify the form or forms of production in which it seeks to have ESI produced. The responding party must also state the form that it intends to use for producing ESI if the requesting party does not specify a form or if the responding party objects to the requested form. If the parties cannot agree the court will resolve the dispute.

#### **For Computer Forensic Professionals:**

- It may be necessary to convert data from legacy systems into a more current data format
- Data cannot be converted from its normal form into a form that makes it more difficult to use. If the data is normally electronically searchable it must remain this way

**\*\*\*Strangely Rule 34 is actually titled "*Production of Documents, Electronically Stored Information and Things and Entry Upon Land for Inspection and Other Purposes*" - recognition that technology is going to change**

**Rule 37(f) Electronically Stored Information** absent exceptional circumstances a court may not impose sanctions on a party for failing to provide ESI lost as a result of routine, good-faith operation of an electronic information system. This is commonly referred to as the "Safe Harbor" rule. This recognizes that some computer systems routinely alter and delete information without specific direction from an operator. A party cannot exploit the routine operation of an information system to thwart discovery by allowing a system to continue to destroy information that it is required to preserve.

A good-faith effort would require a party under "litigation hold" to take steps to prevent further loss of information.

#### **For Computer Forensic Professionals:**

- Litigation Hold is when a party is under a duty to preserve information because of pending or "reasonably anticipated litigation". Intervention in the routine operation that is destroying data would be litigation hold.

**Rule 45 Subpoena** was amended to recognize ESI. Several other key amendments are:

1. ESI can be sought by subpoena
2. a subpoena can designate a form or forms for production of ESI
3. a person receiving the subpoena can object to the forms of production
4. if no forms or production are specified the ESI must be provided in the form in which it is usually maintained or forms that are reasonably usable
5. a person should not have to produce the same ESI in more than one form unless so ordered by the court
6. provides protection for undue impositions on nonparties
7. the party serving the subpoena must avoid imposing undue burden or expense on the person subject to the subpoena
8. a subpoena is available to permit testing and sampling as well as inspection and copying of ESI. This does not create a routine right to direct access to the ESI.
9. assertion of privilege after production of ESI

#### **For Computer Forensic Professionals:**

- It is important that you work with your client on developing a strategy for requesting information and helping them to craft a reasonable request both from a data requested as well as a data received position

## **5. What should a company do if something happens?**

The ABA recommends the following:

1. Locate the ESI including backups and email
2. Collect technical information regarding hardware, software, seasonal data trends, sunset provisions and metadata
3. Collect management information regarding backup, ownership, business use and regulatory requirements
4. Develop a methodology for tracking and collecting changed or new matter-specific ESI
5. ID key players and collection information about how they create, use, store and retain data
6. ID key data types that may be associated and key systems that create the data
7. ID key words and dates
8. ID preferred models for processing, reviewing and producing ESI
9. Anticipate areas of dispute and develop a resolution plan

## **6. What mistakes can be avoided?**

1. Impose proper preservation holds prior to actual litigation
2. Don't claim "Attorney Work Product" when no litigation is anticipated to try and claim protection. This establishes a date that data preservation should have started
3. Get IT personnel involved early in the discovery process
4. Identify accessible and inaccessible ESI prior to litigation

5. Identify ESI that will be automatically deleted prior to litigation
6. Identify key players in litigation early and move to preserve all their storage media
7. You must follow-up with the key players in litigation to ensure they are following the preservation order
8. ESI is going to have to be produced rapidly
9. Don't assume that one data production form is going to work for all ESI
10. Communicate frequently and clearly with everyone involved in the e-discovery process

## **7. What can companies do in advance?**

1. Be proactive. Develop a e-discovery plan for the organization and identify ESI.
2. Develop litigation hold policies. Procedures for notifying personnel of the situation and the what and how of preserving the data.
3. Develop a document retention policy. Companies are not expected to retain every bit of information forever. Rule 37(f) also protects companies from sanctions if ESI becomes unavailable due to the implementation of routine document retention policies. There must also be procedures in-place to halt the retention policy in the event of pending or threatened suit.

## **8. What about data on personally owned computer, PDAs, cellphones, etc.**

This data is available for discovery if it is used in the conduct of your companies business that is part of the e-discovery process.

## References and Acknowledgements

I would like to acknowledge, reference and thank all the attorneys and writers whose works helped me better understand the changes to the Federal Rules of Civil Procedure.

1. [https://www.abanet.org/litigation/standards/docs/ediscovery\\_report.pdf](https://www.abanet.org/litigation/standards/docs/ediscovery_report.pdf)
2. <http://www.abanet.org/lpm/lpt/articles/ftr07043.html>
3. <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1163671528626>
4. <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1156511794320>
5. [http://www.uscourts.gov/rules/EDiscovery\\_w\\_Notes.pdf](http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf)
6. <http://www.informationweek.com/shared/printableArticle.jhtml?articleID=196600853>
7. <http://www.eapdlaw.com/files/News/fc742488-2f0e-4be0-be07-36775b237051/Presentation/NewsAttachment/98f4f4a5-5f3f-4cf5-a976-36eb9cbf4716/Implications%20of%20Electronic%20Data%20Discovery%20for%20Insurers.pdf>
8. <http://www.enterprisestorageforum.com/continuity/features/print.php/3642421>
9. <http://www.enterprisestorageforum.com/continuity/features/print.php/3642421>